3.2t Transcript

In this video we will briefly cover what network function virtualization (NFV) actually is. In essence, this type of virtualisation can split network networking functions into building blocks that can be chained together to create communication services. As the name suggests, this type of functionality relies heavily on virtualization. This enables the decoupling of network functionality in proprietary hardware appliances so that the functionality can be operated on standard hardware. The various for applications for this could be features such as a firewall, deep packet inspection and intrusion prevention systems. Ultimately, this will provide economic benefits to provisioning because it removes the requirement to invest in proprietary purpose-built hardware, thus reducing the amount of space and power requirements were needed for rollout of network management services. The other benefit to such a deployment is the reduction in time required to deploy network services to satisfy ever-changing business requirements. It also allows organisations to test new features without presenting a high-risk environment for the consumer. Usually this functionality will operate in a virtual machine, if you look back at last week’s tutorial, we installed a virtual machine, while the functionality of NSV appliances can be applied to a similar environment. As you can imagine, this allows great flexibility because you are not actually dealing with the real hardware, merely a virtual machine that can be created and destroyed on a as needed basis. As we can run many virtual machines on one system, we can have many NSV features each achieving their own purpose. For example, we may have one virtual machine that deals with routing, another that deals with firewall aspects of the network, and perhaps another that deals with management of the network. There are other elements tied to NFV as well, the virtualisation layer’s is fundamental for virtual computing power, virtual storage and also virtual networks. These three elements are usually tied to the physical elements of the host machine.

Fundamentally, virtualised networks are a process of combining computer hardware and network resources and functionality into a single entity, in what is commonly known as a virtual network. Network virtualisation is reliant on virtualisation of a platform, which will usually rely on resource virtualisation of a host computer. VLANs are one example of a type of virtual network that we see in networks today and they are very common because most devices in an enterprise environment support the use of VLANs so the offer great flexibility. There are two types of network virtualisation that we should be aware about, external virtualisation is the combination of multiple networks, or part of a network into a virtual entity, this is commonly referred to by VLANs. Internal virtualisation combines network functionality to mimic a single physical network, this is based purely on software. An example of this is in a virtualised environment such as VMware workstation where you use your existing network and ensure this network with virtual machines using a network bridge or network address translation-based networking functionality. Another important feature is virtual switching where you can mimic the functionality of a switch in software and connect multiple virtual machines in a common network segment.

Fundamentally, virtual private networks are a way of extending a private network over a public network and allows users to access resources on a remote private network as though they were physically present at that location. Traffic within a VPN tunnel is generally encrypted, therefore protecting the integrity and confidentiality of the data transmitted between source and destination. There are two types of VPN that we commonly see in networks today, the first type is a site to site VPN. This enables organisations to interconnect between a virtual point to point connection across the Internet and enable a virtual private connection between them, so that access of resources between the endpoints is seamless. The other type of VPN commonly seen is the client to site VPN. This enables remote workers to connect to an organisation and therefore allow the user to access local network resources as though they were actually within the organization. This enables many people to work from home because they do not have to be physically present at the workplace to access resources securely. Usually VPN connections are established by using an encrypted layered tunneling protocol, with authentication methods including either a pre-shared key or certificates that are issued by a certificate authority and are digitally signed.